RFID tag security and personal privacy

RFID World

Boston, September 2007

Lee Tien

tien@eff.org

http://www.eff.org

Electronic Frontier Foundation

Outline

- Basic privacy/security issues
- Privacy threat analysis
- Privacy-endangering applications
- State legislation summary
- Technology convergence
- Policy recommendations

Basic RFID security concerns

- Confidentiality
  - – Prevent unauthorized* reading/copying
- Integrity/availability
  - – Prevent modification, spoofing, replay attacks
  - – Prevent deletion of tag data
- Liability for abuse/misuse of tag data?
- *authorized by who?

Security concerns. . . .

- *“Basic RFID technology does not have necessary technological protections to eliminate the risk of terrorists, criminals, or illegal aliens….spoofing or counterfeiting PASS cards to enter the United States undetected.”*

  – Smart Card Alliance

Successful attacks (read, spoof, crack)

- HID cards (2007)
- British e-passport (2006)
- RFID credit cards (2006)
- Sacramento Capitol access cards (2006)
- Human-implantable VeriChip (2006)
- RFID chips in Dutch e-passport (2006)
- Exxon/Mobil SpeedPass, car anti-theft devices (2005)

Fundamental RFID privacy issues

- RF transmissions hard to secure
- RFID tags can hold much information
  - often linked to unique static identifier
- RFID tags often *promiscuous*
  - respond to any compatible reader
- RFID systems are *stealthy*
  - how do ordinary people exert control?*

RFID: two basic privacy threats

- Exposure/leakage of data on chip
  - skimming or eavesdropping
  - personal data or inventorying
- Tracking
  - static/persistent unique ID
  - distinctive *combination* of type IDs
- Exacerbated because you don’t know if you’ve been read. . . .

. . . Enhanced by inference-making

- E.g., associating chip data with other data
  - Corporate, government databases
  - Bluetooth anecdote
- Need not be in real time: if system logs "xy101zzy" now, can get "true name" later

Are the threats real?

- “Read ranges are too short”??
- But DHS, State conceded 1-meter range
- More important: not the right question
  - RSA: attackers don’t need high reliability; “Reading 1% of cards passing by a busy street corner could be good enough for an attacker.”
  - chokepoints (doorways) mean 1-2 feet enough

EFF in good company

- GAO: *“Key privacy concerns include tracking an individual’s movements and profiling an individual’s habits, among others”*
- DHS Privacy and Integrity Committee: *“widespread surveillance of individuals…without their knowledge or consent.”*
- AeA: *“Perversely maximize the possibility… of an illicit actor ‘tracking’ a person at very long ranges… would potentially threaten individual U.S. citizen privacy.”*

Microsoft: “Helen wears a hat”

- Helen wears her hat to Fourth Coffee, which doesn’t bother to read the tags
- But Southridge Video in Blue Yonder Mall has tag readers and poorly trained staff
- Blue Yonder Mall records Helen’s movements in and out of stores
- The data is sold to Tailspin Toys for marketing purposes
- All this data is discoverable (legal sense)
- Is Helen aware of all this?

MS privacy vulnerability summary

Enablers

- Item tagging
- Interoperability
- Broadcast range
- Unique ID
- After-purchase use
- Take into public venues

Threats

- Radio snooping
- Network snooping
- Database cracking
- Database selling

RFID Exacerbations

- Intimacy of data
- Accumulation of data
- Distribution of data
- Data handling by untrained people

Privacy-endangering applications

- Access control (tracking via unique ID)
- Automatic ID: passports, DLs, WHTI card
- Payment: Exxon/Mobil SpeedPass, RFID credit cards
- Transport systems (locational privacy)
  - EZ-Pass, FasTrak
  - Oystercard etc.

Special case —information goods

- Books, CDs, DVDs more sensitive
  - Political, religious, cultural beliefs?
- Ex.: Vienna, Austria Main Library
  - RFID tags placed on more than 240,000 books and 60,000 CDs/DVDs
  - Label contains: ISBN, author, title, location in library, last person who checked it out

Critical case: government applications

- Transport systems, ID cards
  - No choice when government mandates
  - Concern for accountability*
- Likely designed, intended to be:
  - Promiscuous: readable by many sensors
  - Persistent: can’t kill tags
  - Pervasive: tags *and* sensors/readers will proliferate in public places (malls, airports, campuses)

What’s the accountability problem?

- GAO noted lack of privacy discussion in federal RFID decision-making
  - as if deciding to use RFID = deciding to buy new chairs
  - burden should be on government
- Industry seems to have strong ex parte channels into gov’t decisions, with no privacy advocates or even neutral security researchers involved
- We need good public data

Classic case: RFID and US-VISIT

- Process? Public notice very weak on details
- Alternative technologies?
  - key criterion: “no direct action on the part of the traveler” — excludes many techs
  - anti-privacy — where’d that come from?
- Failure after 15-month trial – GAO
  - “performance and reliability problems”
  - At one site RFID readers correctly ID’d 14% of cars but target read rate 70%
  - Cross-read problem hard to fix

More problems

- Supposed advantages often don’t exist
  - speed? Smart Card Alliance challenged throughput improvement of WHTI
  - security? remote capture, replay of Gen 2 tag ID technically straightforward
- RFID passport supposedly protects privacy by having optical swipe of MRZ
  - So what advantage to RFID distance read?

Government *and* business

- Not either/or – we’re seeing alliance of gov’t and commerce
- DoD, transport sector adopting RFID
- Govt not just using but *subsidizing* RFID
  - Scale economies = lower cost
  - Legitimizes RFID use
  - More RFID sensors in everyday life

RFID as privacy pollution

- Classic “social cost” problem -- RFIDs leak
  - – personal information
  - – persistent ID # for association, tracking
- But *worse* than ordinary pollution
  - – don’t know if your data was captured*
  - – “pollution” has value to business, govt**
- So who has incentive to protect privacy?

State legislation summary

- Many pending bills, some enacted laws*
- Main types:
  - Regulating RFID in govt ID
  - Study commissions/task forces
  - Limited authorization for RFID use
  - Disclosure of commercial use
  - Anti-implantation

California bills pending

- 5 bills
  - DL moratorium
  - K-12 moratorium (attendance-taking)
  - Government ID generally
  - Anti-skimming criminal penalties
  - Anti-implant

Why California?: school went too far

- Public school tried to force students to wear RFID badges to ease attendance-taking
  - *“This is a public elementary school, not a prison/continuation school . . . . help us protect our children now, and future students of any school, from this abuse of personal privacy.”*
  - Letter to district superintendent from parents of 2 students at Brittan Elementary School in Sutter, CA (2/2/05)

School district response

- *“Your complaint will be considered … We ask at the bare minimum that you allow your student to continue participating … If not, please understand that the failure to follow the school rules … could lead to your child being disciplined.”*
  - – Letter from school district counsel (2/8/05)

Firestorm of publicity

- *“Treat kids like sheep, with virtual bells around their necks, and pretty soon they'll start acting like them—not like young citizens learning their rights and responsibilities.”*
  - – Editors, San Jose Mercury News (2/11/05)
- *“[T]agging junior high school kids becomes a form of indoctrination into an emerging surveillance society that young minds should be learning to question.”*
  - – Editors, Scientific American (May 2005)

Bigger picture

- *“The envisioned system should … enable the identification, location, and tracking of individuals on school grounds; ideally, visitors and intruders, as well as staff and students. Cooperative identification and tracking is acceptable; however, non-cooperative identification and tracking is desired.”*
  - U.S. Department of Justice, “Solicitation for Concept Papers” re new school ID and tracking systems, 10/5/05

Media gets big picture …

- *“[Some parents in Sutter] realize that unless they protest loudly, other districts and companies will just assume that people think it's no big deal to have their movements monitored and privacy invaded. They're standing up for everyone's rights by refusing to have the wool pulled over their eyes.”*
  - Editors, San Jose Mercury News (2/11/05)

Electronic Frontier Foundation

SB 30 framework

- 3 basic standards for RFID ID cards
  - **Tamper resistance** to prevent duplication, forgery, or cloning of ID
  - **Authentication** to try to ensure that ID document was legitimately issued, isn't cloned, and is authorized to be read.
  - **Notice** to each recipient of RFID-embedded government ID document about RFID technology, privacy and security implications, how they can protect their information.

More protection for some IDs

- IF multiple uses, public schools, public transport, public benefits (e.g. MediCal)
  - secondary verification and identification procedure that doesn’t use radio waves
  - security protections
    - mutual authentication
    - encryption
    - access control protocol

If personal information, then basic +

- robust encryption: prevent unauthorized reading of transmitted information
- mutual authentication: only those supposed to have access to data stored on ID can read it
- consent: ensure that ID cannot be read unless ID's holder specifically authorizes that reading
- notice to ID holder, e.g.:
  - that shields can reduce privacy, security risks
  - of location of intended readers
  - how data collected, stored in DB

Strong support across political spectrum

- ACLU, La Raza, Privacy Rights Clearinghouse
- AARP, Gun Owners of California, Eagle Forum
- O.C. Register - *"a completely reasonable approach … that would make necessary distinctions between beneficial private uses of new technology and mandatory government uses."*
- L.A. Times- *"Simitian is on the right track. Neither government no private industry has given the public much reason to trust their ability to safeguard sensitive personal information."*

Electronic Frontier Foundation

Where SB 30 is now

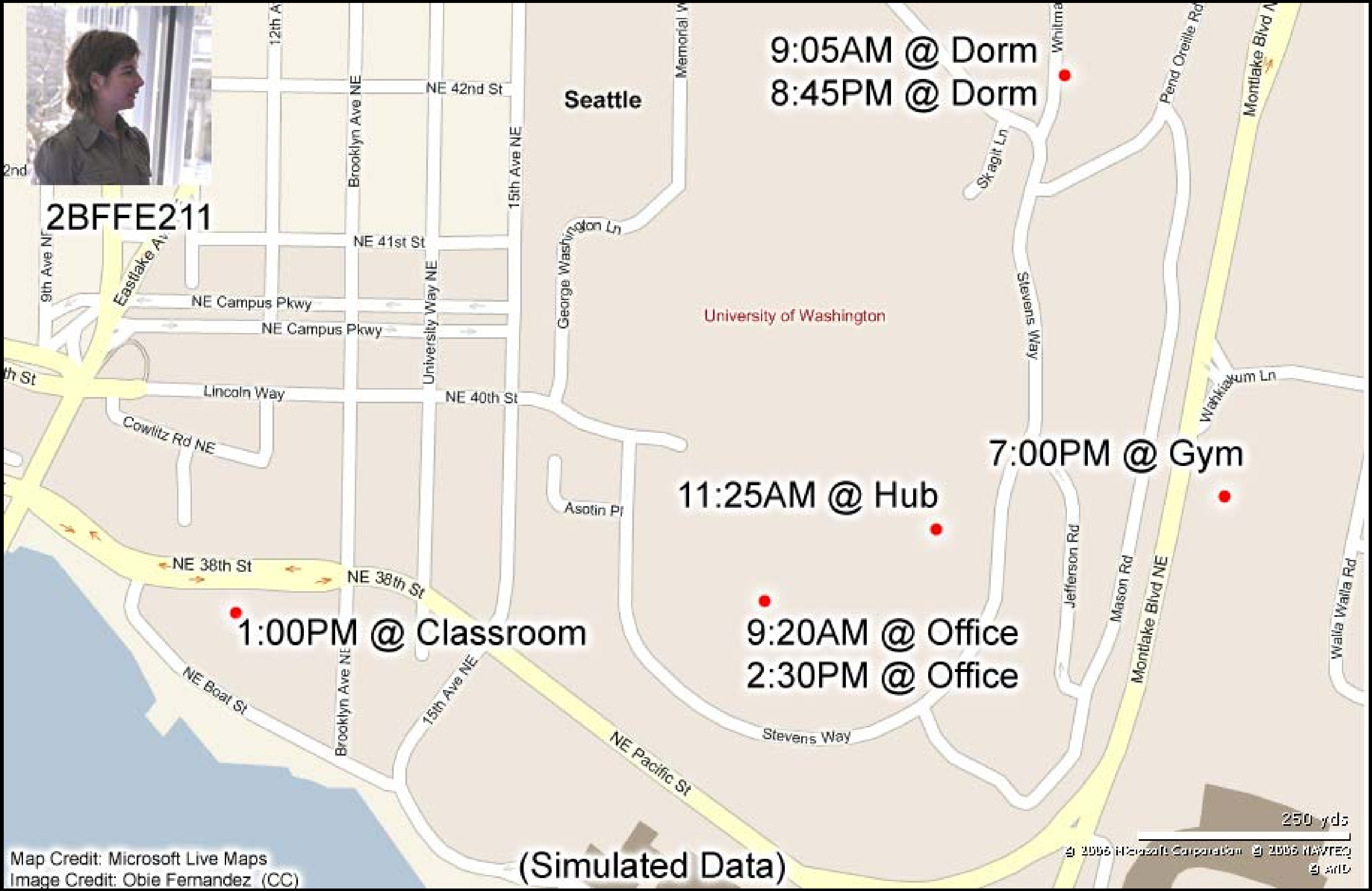
- Last year’s bill (SB 768) passed CA Senate (30-7), Assembly (49-26), but vetoed by governor
- Reintroduced (SB 30), passed Senate 33-3, still moving

Can’t look at RFID alone

- True that RFID merely one of many privacy threats, but that’s cold comfort
- Technologies *combine* in the real world
- Identification: biometrics, RFID
- Location: GPS, videocameras, cellphones
- Data storage: computer databases
- Analysis, profiling: data-mining

"Devices that Tell on You: the Nike+iPod Sport Kit”

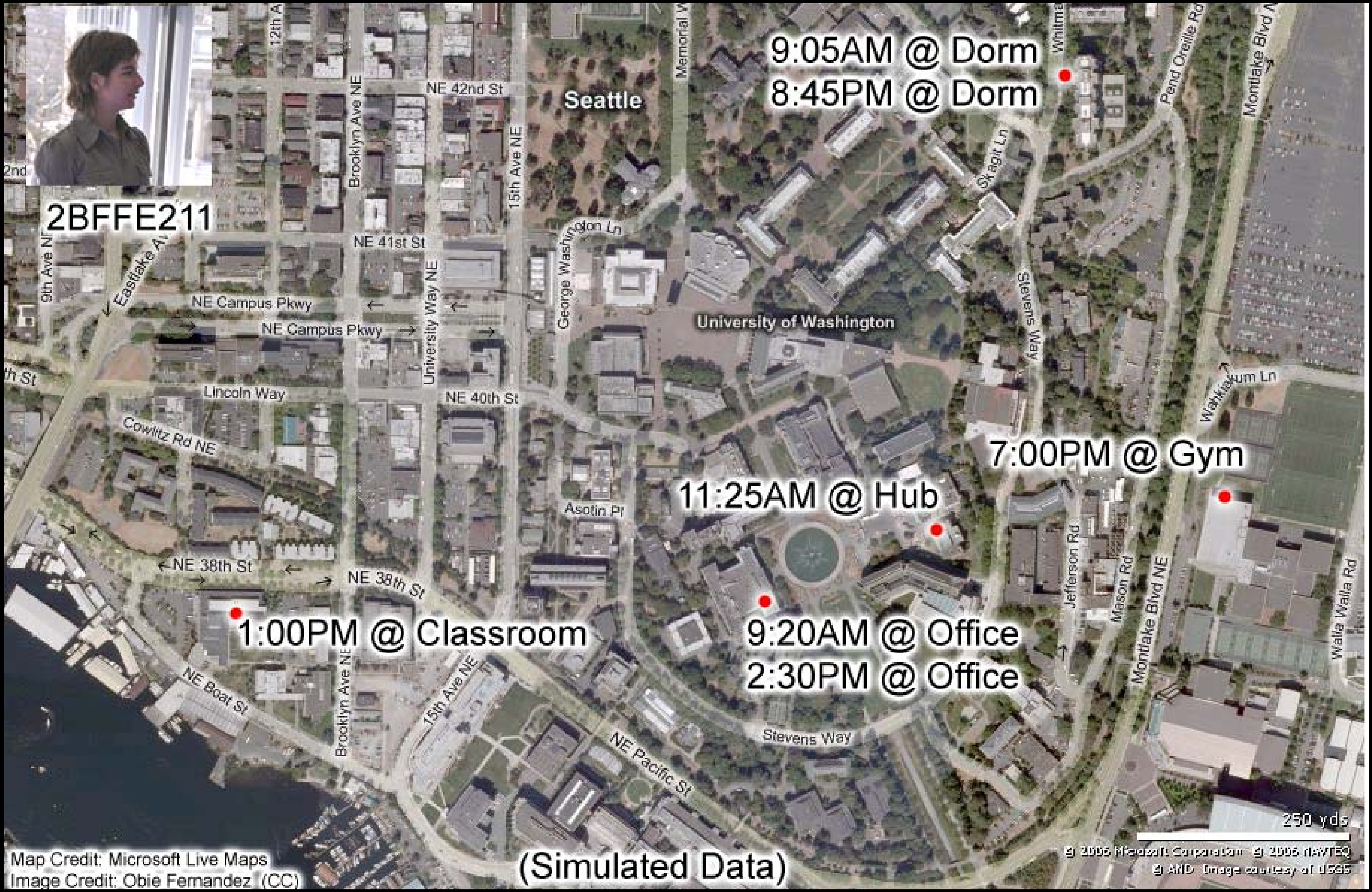
- Kit: shoe chip (size of dinner mint) + receiver (iPod Nano plug-in), records data
- Researchers connected receiver to laptop serial port, wrote app that displayed each device in range (60 feet)
- http://www.cs.washington.edu/research/systems/track.html



(Simulated Data)

Map Credit: Microsoft Live Maps
Image Credit: Obie Fernandez (CC)

Electronic Frontier Foundation



Map Credit: Microsoft Live Maps
Image Credit: Obie Fernandez (CC)

(Simulated Data)

Conclusion

- The privacy and security threats are real
- Aim for consumer/end-user control of RFID
- Laws aren’t enough; build in privacy!
- For now,
  - Kill retail RFID tags at point of sale
  - Don’t use RFID in govt ID or at least use crypto, access controls to mitigate risks
  - Make reading visible/detectable